



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,360	08/31/2000	Leon Wong	418268758US	4462
45979	7590	11/23/2005	EXAMINER	
PERKINS COIE LLP/MSFT P. O. BOX 1247 SEATTLE, WA 98111-1247			ZHONG, CHAD	
			ART UNIT	PAPER NUMBER
			2152	
DATE MAILED: 11/23/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	<p>Application No.</p> <p>09/652,360</p>	<p>Applicant(s)</p> <p>WONG ET AL.</p>	
	<p>Examiner</p> <p>Chad Zhong</p>	<p>Art Unit</p> <p>2152</p>	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 26-50 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 26-50 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ | 6) <input type="checkbox"/> Other: _____ |

FINAL ACTION

1. This action is responsive to communications: Amendment, filed on 09/14/2005.

2. Claims 1-50 are presented for examination. In amendment, filed on 09/14/2005:

Claims 1-25 are Cancelled.

Claims 26 and 29 are amended.

Claims 30-50 are newly added.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371 (c) of this title before the invention thereof by the applicant for patent.

4. Claims 26-33, 35, 38-41, 43, and 46-49 are rejected under 35 U.S.C. 102(e) as being anticipated by Wood et al. (hereinafter Wood), US 6,691,232.

5. As per claim 26, Wood teaches a computer-readable medium having stored thereon a data structure having a plurality of fields, the data structure comprising:

a plurality of client identifier fields (Col. 11, lines 39-41; Fig 4, item 410) that each identify a client computer system that is connected to a server computer system (Col. 11, lines 50-55); and

for each identified client computer system, the data structure further comprising at least one authentication field (Col. 11, lines 40-45) that identifies an authentication method (Col. 11, lines 45-47, Col. 11, lines 53-55 wherein the users get to select an authentication method among a plurality of authentication methods/credential types comprising username/password, onetime passwords, enigma

Art Unit: 2152

challenge, etc) to be used by the server computer system for authenticating the client computer system upon receiving a request from the client computer system for service, the authentication method having been selected based on authentication abilities (Col. 11, lines 53-56, the authentication abilities/authentication methods/credential types are supplied by users, which means the client/user is able to use the supplied credential types. Client is able to use username/password or onetime password as two types of authentication abilities) and access rights (examiner will read access permission as access rights of the client, Col. 13, lines 43-55; Col. 14, lines 30-40, the gatekeeper/entry handler 110 is to determine whether previously authenticated credentials are sufficient for the requested access, the access request may or may not have associated previously authenticated credentials sufficient to support the requested access; session token supplies identity mappings, authorizations, roles, permissions, environmental variables, etc., and is maintained through the credential level change, therefore, the credential types helps the gatekeeper/entry handler determine the access permission of a client; Col. 11, lines 30-35, Col. 12, lines 55-60; Col. 14, lines 7-25, wherein the 'trust level' is the access rights of the client) of the client computer system so that the client computer system need not unnecessarily reveal secret information.

6. As per claim 27, Wood teaches wherein each client identifier field identifies a single client computer system (Col. 11, lines 50-55).

7. As per claim 28, Wood teaches the server computer system has access to the data structure prior to receiving the request from the client computer (Col. 12, lines 25-50).

8. As per claim 29, Wood teaches the data structure is further configured to be altered upon being stored, so as to allow a client computer to use additional authentication methods (Col. 11, lines 30-67).

9. As per claim 30, Wood teaches a method in a server computer of authenticating client computer systems, the method comprising:

receiving from a controlling client computer system (Fig 1, item 170, wherein each client computer system has a browser) an instruction that indicates an authentication methodology that is to be used to authenticate a client computer system (Col. 11, lines 30-67), the authentication methodology being selected from multiple authentication methodologies based on authentication abilities and access rights of the client computer system (Col. 11, lines 30-67); and

upon receiving a request from the client computer system to access a service of the server computer, authenticating the client computer system using the indicated authentication methodology (Col. 12, lines 25-50).

10. As per claim 31, Wood teaches the instruction indicates that multiple authentication methodologies can be used to authenticate the client computer system and wherein the client computer system is authenticated using one of the indicated authentication methodologies (Col. 11, lines 30-67).

11. As per claim 32, Wood teaches the instruction indicates that the authentication methodology is to be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated using the indicated authentication methodology (Col. 7, lines 35-40, wherein plurality of client systems authenticate with the gatekeeper/entry handler component 110).

12. As per claim 33, Wood teaches the instruction indicates multiple authentication methodologies can be used to authenticate multiple client computer systems and wherein the multiple client computer systems are authenticated using one of the indicated authentication methodologies (Col. 7, lines 35-40; Col. 11, lines 30-67, wherein the user/client is allowed to choose credential types to be used to authenticate to the server, all the users can use a particular method of authentication, i.e. certificate authority).

Art Unit: 2152

13. As per claim 35, Wood teaches the authentication methodology is a basic HTTP authentication (Col. 12, lines 25-30).

14. As per claim 38-41, and 43, the claims are rejected for the same reasons as rejection to claims 30-33, and 35 above respectively.

15. As per claims 46-49, the claims are rejected for the same reasons as rejection to claims 30-33 above respectively.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 34, 36-37, 42, 44-45, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wood et al. (hereinafter Wood), US 6,691,232, in view of AAPA (Applicant Admitted Prior Art).

18. As per claims 34 and 42, Wood does not explicitly teach wherein the authentication methodology is an assertion authentication.

However, AAPA discloses of assertion methodology as a way of authenticating between client and server, (see for example, AAPA specification pg 3, lines 1-3). It would have been obvious to one of ordinary skill in this art at the time of invention was made to combine the teaching of Wood and AAPA because the teaching of AAPA to allow assertion would improve the trust in between the two systems, as both

Art Unit: 2152

sides agree to trust each other initially. Furthermore, Wood's system supports plurality of authentication methodologies, it would have been obvious to incorporate assertion method with Wood to improve the functionality of Wood by allowing for more choices for authentication.

19. As per claims 36 and 44 Wood does not explicitly teach wherein the authentication methodology is digest authentication.

However, AAPA discloses of digest method, see for example, pg 3, lines 10-22. It would have been obvious to one of ordinary skill in this art at the time of invention was made to combine the teaching of Wood and AAPA, the rational to combine is discusses in claims 34 and 42 above.

20. As per claims 37 and 45, Wood does not explicitly teach wherein the authentication methodology is an NTLM authentication.

However, AAPA teaches NTLM authentication method, see for example, pg 3, lines 23-24. It would have been obvious to one of ordinary skill in this art at the time of invention was made to combine the teaching of Wood and AAPA, the rational to combine is discusses in claims 34 and 42 above.

21. As per claim 50, the claim is rejected for the same reasons as rejection to combination of claims 34-37 and 42-45 above.

Response to Arguments

22. Applicant's remarks filed 09/14/2005 have been considered but are found not persuasive.

23. In the remarks, Applicant argued in substance that Wood does not teach selecting an authentication methodology based on authentication abilities, and that authentication mechanism for a trust level is selected based on the knowledge of which authentication mechanism a user can support.

Art Unit: 2152

In response to Applicant's arguments, Wood teaches the above limitations. Specifically, referring to Col. 11, lines 30-67, the user has the capability to select a particular type of authentication method to use when attempting to authenticate with the server. The user select from a variety of authentication methodologies, the user selection is realized through interaction with login component 120; furthermore, the user is selecting based on his/her authentication abilities and access rights, in a non-limiting example, the user can select HTTP/login/password option, which means the user/client has the authentication ability to authenticate with the server using said HTTP/login/password option. Therefore, Wood teaches selecting an authentication methodology based on authentication abilities, and that authentication mechanism for a trust level is selected based on the knowledge of which authentication mechanism a user can support.

24. **THIS ACTION IS MADE FINAL.** Applicant is reined of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

25. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following patents and publications are cited to further show the state of the art with respect to

Art Unit: 2152

“Methods and systems for selecting methodology for authenticating computer systems on a per computer system or per user basis”.

- | | | |
|-------|--|-----------------|
| i. | US 6,170,057 | Inoue et al. |
| ii. | US 5,721,780 | Ensor et al. |
| iii. | US 6,470,447 | Lambert et al. |
| iv. | US 6,278,449 | Sugiarto et al. |
| v. | US 6,185, 612 | Jensen et al |
| vi. | US 5,930,804 | Yu et al. |
| vii. | US 5,909,503 | Graves et al. |
| viii. | US 5,875,432 | Sehr. |
| ix. | US 6,446,204 | Pang et al. |
| x. | “SDSS Science Archives Security module API”, Gyula P. Szokoly 1996. | |
| xi. | “Sesame Authentication protocol” | |
| xii. | “Modern Encryption Methods in User Authentication”, Lass Huovinen, 1997 | |
| xiii. | “Integrating Policy-Driven Role Based Access Control Security Architecture”, Along Lin, 1999 | |

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chad Zhong whose telephone number is (571)272-3946. The examiner can normally be reached on M-F 7:15 to 4:30.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, JAROENCHONWANIT, BUNJOB can be reached on (571)272-3913. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available

Art Unit: 2152

through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CZ
October 5, 2005



BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER